UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

United States of America,	)	**CASE NO. 1:16 CR 224**
	)	
Plaintiff,	)	**JUDGE PATRICIA A. GAUGHAN**
	)	
Vs.	)	
	)	
Bogdan Nicolescu, *et al.*,	)	**Order**
	)	
Defendants.	)	

INTRODUCTION

Currently pending is the United States of America's Notice and Motion in Limine Regarding Authentication (Doc. 60). For the reasons that follow, the motion is GRANTED in PART and DENIED in PART. Defendant Danet filed a partial opposition to the government's motion. No other defendant responded.

ANALYSIS

The government moves the Court to find that three classes of evidence qualify as "self authenticating" and that the certificates supplied by the government satisfy the authentication rules. The Court will address each category in turn.

A. Provider records

The government asks that the Court "pre-authenticate" records from the following service providers: America Online; 1&1 Media; Google; Yahoo; Facebook; CentriLogic; and Dreamhost. According to the government, these documents are self-authenticating pursuant to Fed.R.Evid. 902(11) and 902(13). These rules provide as follows:

> (11) Certified Domestic Records of a Regularly Conducted Activity. The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)-(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record–and must make the record and certification available for inspection–so that the party has a fair opportunity to challenge them.
>
> (13) Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

The government filed certifications from the aforementioned providers. Defendant Danet does not dispute that these records are authentic and that the records associated with Exhibit A constitute "business records certified by a qualified witness" pursuant to Fed.R.Evid. 902(11). Defendant simply notes that "attribution" remains in dispute. Because defendant does not dispute authenticity, the Court accepts the certifications as evidence of authenticity and a live witness need not be produced.

Defendant points out that at least one certification set forth in Exhibit B provides that certain records were forwarded directly to the FBI from devices the FBI placed in the provider's datacenters or as a result of software designed to forward traffic to FBI servers. Because the provider did not observe or keep records of this data, it cannot authenticate the documents. With

respect to these documents, the government acknowledges that it must provide testimony from the FBI regarding the FBI's software or the device placed on the provider's datacenter. The Court further notes that any records sent directly to the FBI for which no copy was maintained by the provider must be authenticated by other means. At least one certificate *expressly* provides that the provider cannot authenticate these records. The government provided a supplemental certification from an FBI agent who purports to attest that the FBI software or device implemented in connection with the Bayrob investigation is accurate and reliable. The certification, however, does not speak to any particular documents or the authenticity of those documents. Because there is no certification with respect to these types of documents, Rules 902(11) and (13) do not apply.[1]

B. Drive images

The certifications set forth in Exhibit C are directed at the authenticity of hard drives. According to the certifications, the certifiers were either present when each drive was seized or obtained the drive from the FBI. The certifiers indicate that they made complete and accurate images of the hard drives and that they were qualified to do so. In addition, the certifications

---

[1] Defendant also objects to the "admission or authentication" of any legal process, *i.e.*, search warrants or subpoenas, contained within any of the government's authentication exhibits. In response, the government indicates that it does not intend to introduce any such legal process, except in response to an argument raised by the defendants that the jury cannot determine which provider record is being certified by which certificate. The Court will not rule on this issue at this time. Rather, defendant Danet must notify the government at least 45 days prior to trial as to whether it will object on this basis. If so, the government may refile its motion specifically addressing the authenticity of the legal process at issue.

provide that, with regard to computer or other storage material, the "hash" of the original drive matches the "hash" of the image copy. With respect to cellphones, the examiners relied on specialized software to confirm the accuracy of the image.

In response, defendant makes a number of arguments. Defendant argues that some of the electronic devices at issue were obtained as a result of searches and seizures occurring overseas. As such, there are chain of custody issues, which in turn raise "significant foundational and authentication issues." According to defendant, most of the certifications do not speak to what happened to the electronic device between the time it was seized and the time it arrived at the FBI. In other words, the certifications do not establish chain of custody. Similarly, defendant argues that certain aspects of the certifications go beyond authentication. By way of example, defendant notes that certain statements in the certifications provide that the device was obtained by the certifier, who was present in defendant's apartment. Defendant claims that these statements go beyond the accuracy of the electronic copying and, are therefore, testimonial in nature.

Rule 902(14) provides that the following category of evidence is self-authenticating:

> (14) Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12).

Upon review, the Court finds that the government has established authenticity for the purposes of showing that the digital images at issue are accurate copies of the electronic devices. The Court agrees with defendant, however, that the certifications are not sufficient to establish that a particular piece of electronic equipment was obtained at a particular location. As an initial matter, the Court notes that the majority of the certifications simply provide that the device was

obtained from the FBI. Certainly, additional testimony would be required to establish how the FBI obtained the device in question or where that device came from. The certifications do no such thing. And, with regard to the certifications providing that the certifier obtained a device at a particular location, the Court agrees with defendant that this type of testimony is not the type of information that the rule is intended to cover. Rather, it is testimonial in nature and is not, in and of itself, self-authenticating. However, the government need not call a witness to establish that the images at issue are authentic copies of the materials contained on the electronic devices at issue.[2]

C. Foreign records

The government seeks to authenticate "records provided by the Romanian Government in response to Mutual Legal Assistance Treaty Requests by the United States." The government does not offer even a generic description of this category of documents. At the time the government filed its motion, the government lacked a certification from Romania. It appears, however, that the government came into possession of a certification and, in fact, filed it in connection with its reply brief. In addition, the government acknowledges that some of the

---

[2] The Court rejects any argument by defendant regarding the authenticity of the drives for which the boot process of the operating system was initiated prior to the imaging process. Defendant argues, without explanation, that this "error" may have had an impact on the integrity of the process. The certification defendant cites, however, concludes that the "hash" values are identical and thus demonstrate that the forensic image and the original device are exact copies. The Court finds that this aspect of the certification establishes authenticity and defendant's generic argument to the contrary is insufficient to challenge the conclusion regarding the "hash" values. As noted by the government, the commentary to the rule expressly identifies "hash" values as a way of authenticating copies of electronic media.

records have not yet been received from Romania, although defendant possesses copies of the documents. According to the government, these "documents" are self-authenticating under Fed.R.Evid. 902(11), 902(13), and 18 U.S.C. § 3505.

In response, defendant argues that the government's request is premature. According to defendant, at the time he filed his brief in opposition, no certification existed. Moreover, as the government admitted, it does not have all of the records. As such, the defendant argues that the government's request is premature.

Upon review, the Court denies the government's request to deem the "foreign records" self-authenticating. As an initial matter, neither the government nor the certification describes (even in general terms) the documents that fall within this category. The Court further agrees with defendant that the government certainly cannot ask the Court to authenticate documents it does not even possess yet. Regardless, the Court has reviewed the certification provided by the government and finds that it does not satisfy any of the self-authentication rules or 18 U.S.C. § 3505.

Rule 902(11) is directed at certified domestic records. That provision does not apply to foreign records. Rule 902(13) is entitled "certified records generated by an electronic process or system." That rule, however, requires that the certification comply with either Rule 902(11) or Rule 902(12). Because Rule 902(11) is inapplicable in that it is directed at domestic records, the Court will determine whether the government is able to satisfy Rule 902(12). Upon review, the Court finds that it cannot. Rule 902(12) is directed at certified foreign records of a regularly conducted activity. The rule, however, is expressly limited to civil cases. Thus, because the government is unable to comply with either Rule 902(11) or Rule 902(12), it cannot meet the

requirements of Rule 902(13). Accordingly, the Court turns to whether the certification complies with 18 U.S.C. § 3505. That statute provides as follows:

> § 3505. Foreign records of regularly conducted activity
>
> > (a)(1) In a criminal proceeding in a court of the United States, a foreign record of regularly conducted activity, or a copy of such record, shall not be excluded as evidence by the hearsay rule if a foreign certification attests that--
> >
> > > (A) such record was made, at or near the time of the occurrence of the matters set forth, by (or from information transmitted by) a person with knowledge of those matters;
> > >
> > > (B) such record was kept in the course of a regularly conducted business activity;
> > >
> > > © the business activity made such a record as a regular practice; and
> > >
> > > (D) if such record is not the original, such record is a duplicate of the original;
> >
> > unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.
> >
> > (2) A foreign certification under this section shall authenticate such record or duplicate.

On its face, this statute provides that the hearsay rule shall not exclude certain foreign business records. A certification also serves to satisfy authentication requirements. The certification, therefore, must satisfy the requirements set forth in § 3505(a)(1)(A)-(D). Upon review of the certification provider by the government, the Court finds that it falls short of meeting the certification requirements. The certification provides in relevant part:

> I certify that while executing your request for international judicial assistance, all the documents and information, including the information from our databases available to the Romanian judicial authorities and all the information in electronic format provided to them by the public network providers or communication services, were obtained and filed according to Romanian law, the same way as if they were requested, obtained and filed,

at that specific time, for a case investigated by the Romanian judicial authorities in which I would personally pursue a criminal prosecution.

Simply put, this certification wholly fails to address any of the elements of the statute. And, even if somehow Rule 902(13) applied, this certification falls far short of establishing that the documents–whatever they may be–were prepared by an electronic process or system that produces an accurate result and that such production constitute records of a regularly conducted activity. Accordingly, the Court denies the government's request as it pertains to the authenticity of "foreign records."

CONCLUSION

For the reasons that follow, the government's motion is GRANTED in PART and DENIED in PART as set forth herein.

IT IS SO ORDERED.

/s/ Patricia A. Gaughan
PATRICIA A. GAUGHAN
United States District Judge
Chief Judge

Dated: 5/31/18